GLOBAL CYBER RISK SERVICES

New York Department of Financial Services Registered Requirement & Prohibited Practices for Credit Reporting Agencies

The Regulation:

As part of Governor Cuomo's commitment to protecting users of financial products and services, New York State's Department of Financial Services (NYDFS) has taken additional steps to address identified deficient practices and failures of consumer credit reporting agencies.

Background

On September 18, 2017, NYDFS released a regulation, 23 NYCRR 201, that requires consumer reporting agencies to register with the Superintendent of NYDFS by February 1, 2018 in order to do business with any New York State resident. As part of the new regulation, consumer reporting agencies must establish and maintain a cybersecurity program designed to protect consumers' data and manage cyber while also following the compliance requirements of 23 NYCRR 500.

The new NYDFS regulations are being enacted at a time when NYDFS has issued requirements for cyber security for other types of financial institutions and has identified that New York residents are at risk with consumer credit reporting agencies exercising deficient practices to safeguard consumer data; failure of consumer credit reporting agencies to maintain accurate consumer data; and failure of consumer credit reporting agencies to appropriately investigate consumer disputes of alleged inaccuracies in credit reports.

The Requirements:

In addition to enacting financial based controls, all organizations affected by the regulations will have to achieve certain cybersecurity milestones by established dates, which are different than the already released 23 NYCRR 500 deadlines. Some elements of the cybersecurity and risk management program must be in place by April 4, 2018 once the regulations take effect upon publication of the Notice of Adoption in the State Register. Additional regulatory controls are required to be in effect in October 2018, April 2019 and October 2019. Below is a summary of when each control must be implemented by the covered organization.

Due April 4, 2018:

- Identify a qualified employee or contractor as Chief Information Security Officer (CISO), responsible for overseeing and implementing the cybersecurity program; and
- Initiate a cybersecurity program, starting with access control and required policies and procedures.

Due October 4, 2018:

- The appointed CISO shall report in writing annually to the board of directors on the topic of material risks;
- Implement a monitoring and testing program to assess the cybersecurity program; and
- Add regular cybersecurity training for personnel.

Due April 4, 2019:

- The organization's cybersecurity program will have written and approved procedures and policies regarding secure development practices for in-house developed applications;
- The organization shall securely manage the disposal of nonpublic information once it is deemed no longer necessary for business purposes; and
- The organization shall implement controls, including encryption, to protect nonpublic information held or transmitted by the organization, while in transit or at rest.

Due October 4, 2019:

- The organization shall have written policies and procedures governing third party providers' systems which access or store nonpublic information.

The Solution:

We believe that NYDFS has taken the right steps in establishing baseline criteria for protecting New York residents from deficient cyber security programs in organizations that use New York resident information. Organizations affected by these new regulations hopefully already have measures like these in place and may simply require additional enhancements or oversight. However, for those that do not have a mature cyber risk program, and would like to move towards compliance, we offer the Cyber Operational Risk Management program.

Alvarez & Marsal's (A&M) Cyber Operational Risk Management program helps organizations understand their current cyber risk maturity level with respect to the new regulation and helps them develop a roadmap to ensure each control is successfully implemented by the required dates.

The A&M Cyber Risk team, in collaboration with your executive management and information security teams, will help address your organization's compliance with NYDFS regulations through one or more of the following services:

- Providing an experienced, qualified individual to act as the CISO responsible for overseeing and implementing the required cybersecurity program;
- Developing and providing some or all of the written policies and procedures as required by NYDFS;
- Providing a gap analysis identifying what sections of the NYDFS regulation are currently in place, covered by other industry/ government regulations or not implemented;
  Providing a comprehensive risk assessment of information systems to enhance or develop the cybersecurity program;
- Aligning the cybersecurity program with the organization's approach to risk management; and
- Developing a cybersecurity roadmap that will provide an approach to meet all NYDFS requirements within the timelines dictated by the NYDFS.

A&M's Cyber and Operational Risk Management Approach

A&M brings a deep operational heritage and hands-on approach to delivering cybersecurity solutions that create sustainable operational, regulatory and financial results. Our Cyber Risk Team are senior professionals uniquely qualified with regulatory and industry experience to address the demands of organizations and to manage cyber and operational risks in a comprehensive manner.

A&M's approach focuses on providing foundational solutions that mitigate risk and ensure appropriate levels of capital reserves while maximizing operational effectiveness. We provide an integrated strategy that addresses and manages the full spectrum of threats posed by the dynamic operational and cyber risk landscape.

Contact Us

Global Cyber Risk Services
+1 212 763 1958 (New York)
+1 202 688 4280 (Washington, D.C.)
gcrs@alvarezandmarsal.com

A&M's Global Cyber Risk Services team has extensive experience in designing, developing, and implementing effective and sustainable programs. Our seasoned cyber professionals have sat in your chair and possess the right blend of technical and business savvy. Our team has decades of government and private sector experience, which includes defending individuals, companies, and nations against the most sophisticated cyber adversaries. We work as advisers, interim leaders, and partners who not only tell you what you need to know, but will work side by side with you to achieve your objectives

When action matters, find us at:
www.alvarezandmarsal.com

Follow us on:

About Alvarez & Marsal

Companies, investors and government entities around the world turn to A&M when conventional approaches are not enough to activate change and achieve results.

Privately held since 1983, A&M is a leading global professional services firm that delivers performance improvement, turnaround management and business advisory services to organizations seeking to transform operations, catapult growth and accelerate results through decisive action. Our senior professionals are experienced operators, world-class consultants and industry veterans who draw upon the firm's restructuring heritage to help leaders turn change into a strategic business asset, manage risk and unlock value at every stage.

ALVAREZ & MARSAL